PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 30 March 2001 (30.03.01)	
International application No. PCT/EP00/07122	**Applicant's or agent's file reference** K 51 511/7ch
International filing date (day/month/year) 25 July 2000 (25.07.00)	**Priority date** (day/month/year) 30 July 1999 (30.07.99)
Applicant MÖDL, Albert et al	

1. The designated Office is hereby notified of its election made:

   [X] in the demand filed with the International Preliminary Examining Authority on:

   06 February 2001 (06.02.01)

   [ ] in a notice effecting later election filed with the International Bureau on:

   _____

2. The election [X] was

   [ ] was not

   made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Nestor Santesso
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5
K 51 511/7ch		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	(Frühestes) Prioritätsdatum *(Tag/Monat/Jahr)*
PCT/EP 00/ 07122	25/07/2000	30/07/1999
Anmelder		
GIESECKE & DEVRIENT GMBH		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

[X] Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. **Grundlage des Berichts**

   a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

   [ ] Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

   b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

   [ ] in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

   [ ] zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

   [ ] bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

   [ ] Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

   [ ] Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. [ ] **Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen** (siehe Feld I).

3. [ ] **Mangelnde Einheitlichkeit der Erfindung** (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

   [X] wird der vom Anmelder eingereichte Wortlaut genehmigt.

   [ ] wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

   [ ] wie vom Anmelder vorgeschlagen [ ] keine der Abb.

   [X] weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

   [ ] weil diese Abbildung die Erfindung besser kennzeichnet.

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
[redacted]EP 00/07122

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G07F7/10 G07C9/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 G07F G07C

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)
EPO-Internal, WPI Data, PAJ

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	US 5 208 447 A (KRUSE DIETRICH) 4. Mai 1993 (1993-05-04) Zusammenfassung Spalte 2, Zeile 46 -Spalte 3, Zeile 36 ---	1-9
Y	US 5 239 166 A (GRAVES MARCEL A) 24. August 1993 (1993-08-24) Zusammenfassung Spalte 3, Zeile 46 -Spalte 4, Zeile 19; Anspruch 1 ---	1-9
A	US 5 721 781 A (DEO VINAY ET AL) 24. Februar 1998 (1998-02-24) Zusammenfassung Spalte 9, Zeile 49 -Spalte 10, Zeile 30; Abbildungen 7,8 --- -/--	1-3

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

[X] Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :
"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist
"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist
"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden
"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist
"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
27. Oktober 2000	03/11/2000

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Teutloff, H

1

Formblatt PCT/ISA/210 (Blatt 2) (Juli 1992)

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
[redacted]/EP 00/07122

C.(Fortsetzung) ALS WESENTLICH AN[redacted]EHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 875 868 A (PITNEY BOWES) 4. November 1998 (1998-11-04) -----	

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
[redacted]/EP 00/07122

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5208447 A	04-05-1993	AT 109293 T	15-08-1994
		DE 59006559 D	01-09-1994
		EP 0400441 A	05-12-1990
		ES 2057264 T	16-10-1994
US 5239166 A	24-08-1993	CA 1326304 A	18-01-1994
		AT 125054 T	15-07-1995
		AU 633534 B	04-02-1993
		AU 4781590 A	26-07-1990
		DE 69020746 D	17-08-1995
		EP 0379333 A	25-07-1990
		JP 2271466 A	06-11-1990
		NZ 232106 A	26-05-1993
		NZ 244768 A	26-05-1993
US 5721781 A	24-02-1998	NONE	
EP 0875868 A	04-11-1998	CA 2231210 A	04-09-1998

T. 15

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

PCT

(Artikel 36 und Regel 70 PCT)

Aktenzeichen des Anmelders oder Anwalts	WEITERES VORGEHEN	siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)
K 51 511/7 so		
Internationales Aktenzeichen	Internationales Anmeldedatum *(Tag/Monat/Jahr)*	Prioritätsdatum *(Tag/Monat/Tag)*
PCT/EP00/07122	25/07/2000	30/07/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G07F7/10		
Anmelder GIESECKE & DEVRIENT GMBH et al.		

1. Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.

2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.

   ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

   Diese Anlagen umfassen insgesamt 8 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

   - I ☒ Grundlage des Berichts
   - II ☐ Priorität
   - III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
   - IV ☐ Mangelnde Einheitlichkeit der Erfindung
   - V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
   - VI ☐ Bestimmte angeführte Unterlagen
   - VII ☐ Bestimmte Mängel der internationalen Anmeldung
   - VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags	Datum der Fertigstellung dieses Berichts
06/02/2001	01.08.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde: Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Königer, A Tel. Nr. +49 89 2399 2260

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP00/07122

I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigefügt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-5	eingegangen am	04/07/2001	mit Schreiben vom	04/07/2001

Patentansprüche, Nr.:

1-9	eingegangen am	04/07/2001	mit Schreiben vom	04/07/2001

Zeichnungen, Blätter:

1/1	ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

   Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
   - ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
   - ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

   - ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
   - ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
   - ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
   - ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
   - ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

   (Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen;sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja:	Ansprüche	1-3,5,6,8,9
	Nein:	Ansprüche	4,7
Erfinderische Tätigkeit (ET)	Ja:	Ansprüche	
	Nein:	Ansprüche	1-9
Gewerbliche Anwendbarkeit (GA)	Ja:	Ansprüche	1-9
	Nein:	Ansprüche	

2. Unterlagen und Erklärungen
   siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1) Es wird auf die folgenden Dokumente verwiesen:
   D1: US-A-5 239 166 (GRAVES MARCEL A) 24. August 1993 (1993-08-24)
   D2: US-A-5 208 447 (KRUSE DIETRICH) 4. Mai 1993 (1993-05-04)

2) Unabhängiger Anspruch 1

Dokument D1, das als nächstliegender Stand der Technik angesehen wird, offenbart (vgl. Spalte 3, Zeile 46 - Spalte 4, Zeile 18) ein Verfahren zum Authentisieren eines Benutzers eines Datenträgers (4) zur berechtigten Benutzung des Datenträgers und zum Authentisieren eines Datenträgerendgerätes (3) zum berechtigten Zugreifen des Datenträgerendgerätes auf Speicherbereiche des Datenträgers, umfassend folgenden Schritte:
- Präsentieren eines biometrischen Merkmals eines Benutzers (Spalte 4, Zeilen 8-9),
- Vergleichen des präsentierten biometrischen Merkmals mit einem auf dem Datenträger (4) gespeicherten biometrischen Merkmal (Spalte 4, Zeilen 5-11),

von dem sich der Gegenstand des Anspruchs 1 dadurch unterscheidet, daß zu Beginn folgende Schritte ausgeführt werden:

- Auslesen eines Geheimcodes von dem Datenträger durch das Datenträgerendgerät, wobei der Geheimcode in einem nur für autorisierte Datenträgerendgeräte zugreifbaren Speicherplatz gespeichert ist und / oder nur von einem autorisierten Datenträgerendgerät korrekt entschlüsselt werden kann,
- Präsentieren des ausgelesenen Geheimcodes gegenüber dem Benutzer.

Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, daß ein alternatives Verfahren zur Authentisierung eines Benutzers eines Datenträgers zur berechtigten Benutzung des Datenträgers und zum Authentisieren eines Datenträgerendgerätes, welche direkt vom Benutzer kontrolliert /durchgeführt werden kann, bereitgestellt wird.

In Dokument D1 findet ebenfalls eine Authentisierung des Datenträgerendgerätes statt, jedoch wird diese von der Datenträger und dem Datenträgerendgerät selbständig ausgeführt. Die Merkmale a) Auslesen eines Geheimcodes aus einem für autorisierte Datenträgerendgeräte zugreifbaren Speicherplatz und b) Präsentieren dieses Codes gegenüber dem Benutzer wurden jedoch schon für denselben Zweck bei einem ähnlichen Verfahren zur Authentisierung von Benutzer und Datenträgerendgerät benutzt, vgl. dazu Dokument D2, insbesondere Spalte 2, Zeile 46 bis Spalte 3, Zeile 36. Wenn der Fachmann den gleichen Zweck bei einem Verfahren zur Authentisierung von Benutzer und Datenträgerendgerät gemäß dem Dokument D1 erreichen will, ist es ihm ohne weiteres möglich, die Merkmale mit entsprechender Wirkung auch beim Gegenstand von D1 anzu- wenden. Auf diese Weise würde er ohne erfinderisches Zutun zu einem Verfahren zur Authentisierung von Benutzer und Datenträgerendgerät gemäß dem Anspruch 1 gelangen.

Der Gegenstand des Anspruchs 1 beruht daher nicht auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT).

3) Unabhängiger Anspruch 4

Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 4 angesehen. Es offenbart (die Verweise in Klammern beziehen sich auf dieses Dokument):
Datenträger (4) zur Authentisierung eines Endgeräts gegenüber einem Benutzer und des Benutzers gegenüber dem Datenträger, umfassend
- einen ersten Speicherbereich, in dem ein Geheimcode derart abgespeichert ist, daß der Geheimcode von einem autorisierten Datenträgerendgerät (3) auslesbar (6) und anzeigbar (5) ist (Spalte 4, Zeilen 9-11), und
- einen zweiten Speicherbereich, in dem biometrische Daten abgespeichert sind (Spalte 4, Zeilen 5-9).

Der Gegenstand des Anspruchs 4 ist daher nicht neu (Artikel 33(2) PCT).

3.1) Selbst falls eine besondere Teilung bzw. Gestaltung der beiden Speicherbereiche beabsichtigt sein sollte, ist der Gegenstand als nicht erfinderisch anzusehen

(Artikel 33(3) PCT), da auf dem Gebiet der Chipkarten- und Sicherheitstechnologie dem Fachmann vielfältige vorteilhafte Ausgestaltungen und die gezielte Verwendung separater Speicherbereiche wohlbekannt sind.

4) Unabhängiger Anspruch 7

Das Dokument D1 wird als nächstliegender Stand der Technik gegenüber dem Gegenstand des Anspruchs 7 angesehen. Es offenbart (die Verweise in Klammern beziehen sich auf dieses Dokument):
Authentisierungssystem (siehe Spalte 3, Zeile 46 bis Spalte 4, Zeile 18 und Fig. 1) umfassend einen Datenträger (4) mit Speicherbereichen und ein Datenträgerendgerät (3) zum Zugreifen auf die Speicherbereiche des Datenträgers, dadurch gekennzeichnet, daß
- der Datenträger (4) einen ersten Speicherbereich für die Speicherung eines Geheimcodes und einen zweiten Speicherbereich für die Speicherung biometrischer Daten (Spalte 4, Zeilen 5-11),
- das Datenträgerendgerät (3) eine erste Einrichtung, die zum Auslesen (6) des Geheimcodes aus dem ersten Speicherbereich autorisiert ist sowie zum Präsentieren (5) des ausgelesenen Geheimcodes auf einem Display, und eine zweite Einrichtung zum Einlesen biometrischer Daten (7), und
- eine Einrichtung zum Vergleichen (9) der eingelesenen biometrischen Daten mit im zweiten Speicherbereich gespeicherten biometrischen Daten im Datenträger (4) und/oder im Datenendgerät (3) aufweist (siehe auch Spalte 4, Zeilen 5-11).

Der Gegenstand des Anspruchs 7 ist daher nicht neu (Artikel 33(2) PCT).

4.1) Wie schon in Abschnitt 3.1 erläutert kann auch eine besonders ausgeführte Teilung und Gestaltung der beiden Speicherbereiche nicht als erfinderisch angesehen werden. Ebenso ist eine im Rahmen üblichen Handelns liegende Variation oder Ausgestaltung des Geheimcodes (Geheimzahl, Zufallszahl, PIN, etc.) nicht als erfinderisch anzusehen (Artikel 33(3) PCT).

5) Abhängige Ansprüche 2-3, 5-6 und 8-9

Die abhängigen Ansprüche 2-3, 5-6 und 8-9 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf Neuheit bzw. erfinderische Tätigkeit

erfüllen. Die Gründe dafür sind die folgenden:

5.1) Ansprüche 2, 5 und 8: Die zusätzliche Verwendung einer persönlichen Geheimzahl (PIN) neben der Erfassung biometrischer Merkmale zur Authentisierung eines Benutzers eines Datenträgers ist bereits in Dokument D1 vorgeschlagen worden (siehe Spalte 4, Zeilen 9-11).

5.2) Ansprüche 3, 6 und 9: Bei der Verwendung des Fingerabdrucks eines Benutzers als biometrisches Merkmal handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde, um die gestellte Aufgabe zu lösen. In Dokument D1 wird bereits explizit die Verwendung von Fingerabdruckdaten in einem ähnlichen System und Verfahren vorgeschlagen.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

6) Das mit dem Schreiben vom 04.07.2001 eingereichte Merkmal der Verwendung eines **autorisierten** Datenträgerendgerätes ist nicht klar definiert (Artikel 6 PCT) und trägt nicht dazu bei, daß der Gegenstand der unabhängigen Ansprüche neu bzw. erfinderisch wird.
Die bloße Einführung des Begriffes **autorisiertes** Datenträgerendgerät macht selbst in Kombination mit der Beschreibung nicht klar in welcher Weise und mit welchen technischen Mitteln sich ein solches **autorisiertes** Datenendgerät von anderen Datenträgerendgeräten unterscheiden soll. So wie der Wortlaut momentan zu verstehen ist, fallen alle Datenträgerendgeräte, die dazu geeignet oder eingerichtet sind den Datenträger auszulesen in die Kategorie **autorisiertes** Datenträgerendgerät. Wie dem Fachmann außerdem bekannt ist, wird außerdem in vielen Anwendungsfällen vor dem Auslesen eine Kompatibilitätsprüfung zwischen Datenträger und Datenträgerendgerät durchgeführt. Ein positives Ergebnis einer solchen Prüfung, ist ebenfalls als Autorisierung eines Datenträgerendgerätes anzusehen. Das Merkmal eines autorisierten Datenträgerendgerätes bietet somit keine zusätzlichen technischen Merkmale, welche zur Abgrenzung der zitierten Systeme und Verfahren aus D1 bzw. D2 herangezogen werden könnten.

Verfahren, Datenträger sowie System zur Authentisierung eines Benutzers und eines Endgeräts

Die vorliegende Erfindung betrifft allgemein die Authentisierung bei der Benutzung von Datenträgern wie Chipkarten und dergleichen, und insbesondere ein Authentisierungsverfahren, einen Datenträger sowie ein Authentisierungssystem umfassend einen Datenträger und ein Endgerät (Terminal).

Zum Nachweis, daß ein Benutzer zur Benutzung einer Chip- oder Magnetstreifenkarte tatsächlich berechtigt bzw. autorisiert ist, dient üblicherweise eine individuelle Geheimzahl, beispielsweise eine sogenannte PIN (Persönliche Identifizierungs Nummer). Die PIN ist auf der Karte gespeichert und wird, nachdem die Karte in ein Endgerät eingeführt worden ist, mit der dem Endgerät von dem Benutzer angegebenen PIN verglichen. Ist der Vergleich positiv, so kann vom Endgerät z. B. auf geschützte Bereiche der Chipkarte, beispielsweise Speicherbereiche, zugegriffen werden.

Die Benutzung von PINs ist problematisch, weil die Karte in Kenntnis der PIN von jedermann benutzt werden kann. Die Karte ist also nicht an den eigentlichen Karteninhaber, sondern an den PIN-Inhaber gebunden. Durch freiwillige oder unfreiwillige Weitergabe der PIN ist somit ein Mißbrauch der Karte möglich. PINs sind auch insofern unsicher, als sie einerseits vergessen und andererseits ausgespäht werden können.

Selbst wenn sich ein berechtigter Benutzer durch Eingabe seiner PIN ausgewiesen hat, ist das System nur teilweise autorisiert - nämlich der Benutzer gegenüber der Karte beziehungsweise dem Endgerät. Eine Autorisierung des Endgeräts gegenüber der Karte oder dem Benutzer findet nicht statt. Handelt es sich um ein gefälschtes Endgerät, so besteht die Gefahr, daß die PIN mittels dem gefälschten Endgerät ausgespäht wird. Die PIN allein stellt

daher keine ausreichende Sicherung dar, weil eine Authentisierung des Endgeräts gegenüber der Karte bzw. gegenüber dem Benutzer fehlt.

Aus US 5,239,166 ist ein System für einen sicheren Datenaustausch, bestehend aus einer Karte und einem Terminal, bekannt. Bei dem bekannten System überprüfen sich Karte und Terminal gegenseitig. Der Benutzer der Karte wird mittels biometrischer Merkmale, z. B. einem Fingerabdruck, überprüft.

Aus US 5,208,447 ist ein Verfahren zur Überprüfung von Terminals mit einer Chipkarte bekannt, bei dem ein in der Chipkarte gespeichertes Kennwort sowohl verschlüsselt als auch unverschlüsselt an das Terminal gesendet wird. Das verschlüsselte Kennwort wird im Terminal entschlüsselt und mit dem unverschlüsselt gesendeten Kennwort verglichen. Stimmt das entschlüsselte Kennwort mit dem unverschlüsselten Kennwort überein, handelt es sich um ein berechtigtes Terminal.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, den Authentisierungsvorgang sicherer zu gestalten. Insbesondere besteht die der Erfindung zugrunde liegende Aufgabe darin, ein Authentisierungsverfahren, ein Authentisierungssystem bestehend aus Datenträger und Endgerät und einen Datenträger zur Authentisierung sowohl des Benutzers als auch des Terminals vorzuschlagen, wodurch die individuelle Berechtigung des Benutzers und die Echtheit des Terminals überprüfbar sind.

Diese Aufgabe wird erfindungsgemäß durch ein Authentisierungsverfahren, einen Datenträger und ein Authentisierungssystem gemäß den nebengeordneten Ansprüchen gelöst.

In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung angegeben.

Der erfindungsgemäßen Lösung liegt der Gedanke zugrunde, daß der Authentisierungsvorgang sicherer gestaltet werden kann, wenn zunächst die Echtheit des Terminals geprüft wird und dem Terminal anschließend biometrische Daten des Benutzers präsentiert werden. Biometrische Daten, wie ein Fingerabdruck oder dergleichen, sind im Gegensatz zu einer PIN eindeutig benutzerspezifisch. Durch das vorherige Prüfen der Echtheit des Terminals wird gewährleistet, daß ein Ausspähen der sensiblen, benutzerspezifischen biometrischen Daten verhindert wird. Das Prüfen der Echtheit des Endgeräts geschieht in der Weise, daß ein auf dem Datenträger fest gespeicherter Geheimcode, der nur dem Benutzer bekannt ist, von dem Endgerät ausgelesen und dem Benutzer angezeigt wird. Nur wenn der Geheimcode korrekt angezeigt wird, wird der Benutzer dem Endgerät das biometrische Merkmal präsentieren, um sich gegenüber dem Endgerät bzw. dem Datenträger als berechtigter Benutzer auszuweisen. Der Geheimcode kann auf dem Datenträger auf einem nur durch autorisierte Endgeräte zugreifbaren Speicherplatz gespeichert sein und/oder nur von einem autorisierten Endgerät korrekt entschlüsselt werden.

Nachdem die Authentisierung des Terminals erfolgt ist, wird durch Präsentieren des benutzerspezifischen biometrischen Merkmals und Vergleich der von dem biometrischen Merkmal erfaßten Daten mit auf dem Datenträger gespeicherten biometrischen Daten, im Gegensatz zum PIN-Vergleich, eine benutzerindividuelle Authentisierung gegenüber dem Datenträger bzw. dem Endgerät erreicht.

Zusätzlich zur biometrischen Authentisierung des Benutzers kann eine PIN-Authentisierung des Benutzers durch Eingabe einer PIN und Vergleich der eingegebenen PIN mit auf dem Datenträger gespeicherter PIN erfolgen.

Die Erfindung wird nachfolgend beispielhaft anhand der einzigen Figur dargestellt.

Der in der Figur dargestellte Authentisierungsvorgang umfaßt drei Schritte, von denen der zweite Schritt auch entfallen kann.

Im ersten Schritt liest ein Endgerät T (Terminal) von einem ersten Speicherbereich eines Datenträgers C, beispielsweise einer Chipkarte, einen Geheimcode (CODE) aus und präsentiert diesen CODE dem Benutzer U (User). Der CODE ist auf der Chipkarte C beispielsweise auf einem zugriffsgeschützten Speicherplatz und/oder in verschlüsselter Form abgespeichert, so daß der CODE nur von einem "echten" Terminal T, das entweder zugriffsberechtigt ist oder den Entschlüsselungsalgorithmus kennt, ausgelesen und dem Benutzer U angezeigt werden kann.

Wenn der Benutzer U den von dem Terminal T ausgelesenen CODE als seinen Geheimcode wiedererkennt, wird er die weiteren Authentisierungsschritte vornehmen. Im dargestellten Fall wird er dem Terminal T zunächst seine PIN angeben. Die PIN wird dann, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet, wo sie entschlüsselt und mit einer auf der Chipkarte C abgespeicherten PIN verglichen wird, und dem Terminal T wird anschließend das Ergebnis des Vergleichs mitgeteilt. Der Datentransfer, insbesondere der Transfer des CODE's, der PIN und der nachfolgend noch zu beschreibenden biometrischen Daten BIO erfolgt vorzugsweise

in verschlüsselter Form, um ein Ausspähen dieser sensiblen Daten zu erschweren.

Sofern der PIN-Vergleich positiv war ("OK"), führt das Terminal T den Authentisierungsprozeß fort, indem nunmehr die benutzerindividuelle Authentisierung mittels biometrischer Merkmale des Benutzers erfolgt. Dazu präsentiert der Benutzer dem Terminal T ein biometrisches Merkmal, beispielsweise einen Fingerabdruck oder die Iris eines Auges. Das biometrische Merkmal wird vom Terminal T erfaßt und in biometrische Daten BIO umgewandelt, die, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet werden. Dort werden die eingelesenen biometrischen Daten des Benutzers mit auf der Chipkarte C gespeicherten biometrischen Daten verglichen. Im Falle eines positiven Vergleichs ("OK") wird das Terminal T für die Eingabe weiterer Benutzerkommandos freigegeben.

Patentansprüche

1. Verfahren zum Authentisieren eines Benutzers (U) eines Datenträgers (C) zur berechtigten Benutzung des Datenträgers und zum Authentisieren eines Datenträgerendgerätes (T) zum berechtigten Zugreifen des Datenträgerendgerätes auf Speicherbereiche des Datenträgers, umfassend folgenden Schritte:

- Auslesen eines Geheimcodes (CODE) von dem Datenträger (C) durch das Datenträgerendgerät (T), wobei der Geheimcode (CODE) in einem nur für autorisierte Datenendgeräte (T) zugreifbaren Speicherplatz gespeichert ist und/oder nur von einem autorisierten Datenendgerät (T) korrekt entschlüsselt werden kann,
- Präsentieren des ausgelesenen Geheimcodes (CODE) gegenüber dem Benutzer (U),
- Präsentieren eines biometrischen Merkmals (BIO) eines Benutzers (U),
- Vergleichen des präsentierten biometrischen Merkmals (BIO) mit einem auf dem Datenträger (C) gespeicherten biometrischen Merkmal.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß dem Terminal (T) desweiteren eine PIN präsentiert wird, die mit einer auf dem Datenträger (C) gespeicherten PIN verglichen wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß als biometrisches Merkmal (BIO) ein Fingerabdruck eines Benutzers (U) verwendet wird.

4. Datenträger (C) zur Authentisierung eines Endgeräts gegenüber einem Benutzer und des Benutzers gegenüber dem Datenträger, umfassend einen ersten Speicherbereich, in dem ein Geheimcode (CODE) derart abgespeichert ist, daß der Geheimcode von einem autorisierten Datenträgerendgerät (T) auslesbar und/oder entschlüsselbar sowie anzeigbar ist, und einen zweiten Speicherbereich, in dem Daten abgespeichert sind, die der Authentisierung des Benutzers gegenüber dem Endgerät dienen.

5. Datenträger nach Anspruch 4, **dadurch gekennzeichnet,** daß in einem dritten Speicherbereich eine PIN abgespeichert ist.

6. Datenträger nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet,** daß durch biometrischen Daten durch einen Fingerabdruck generiert werden.

7. Authentisierungssystem umfassend einen Datenträger (C) mit Speicherbereichen und ein Datenträgerendgerät (T) zum Zugreifen auf die Speicherbereiche des Datenträgers, **dadurch gekennzeichnet,** daß

- der Datenträger (C) einen ersten Speicherbereich für die Speicherung eines Geheimcodes (CODE) und einen zweiten Speicherbereich für die Speicherung biometrischer Daten,
- das Datenträgerendgerät (T) eine erste Einrichtung, die zum Auslesen des Geheimcodes (CODE) aus dem ersten Speicherbereich authorisiert ist und/oder zum Entschlüsseln des ausgelesenen Geheimcodes (CODE) sowie zum Präsentieren des ausgelesenen Geheimcodes auf einem Display, und eine zweite Einrichtung zum Einlesen biometrischer Daten (BIO), und

- eine Einrichtung zum Vergleichen der eingelesenen biometrischen Daten (BIO) mit im zweiten Speicherbereich gespeicherten biometrischen Daten im Datenträger (C) und/oder im Datenendgerät (T).

aufweist.

8. Authentisierungssystem nach Anspruch 7, **dadurch gekennzeichnet,** daß der Datenträger (C) einen dritten Speicherbereich für die Speicherung einer PIN aufweist.

9. Authentisierungssystem nach Anspruch 7 oder 8, **dadurch gekennzeichnet,** daß die gespeicherten biometrischen Daten durch einen Fingerabdruck generiert werden.

Translation
10/030162
5000

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference K 51 511/7ch	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/EP00/07122	International filing date (*day/month/year*) 25 July 2000 (25.07.00)	Priority date (*day/month/year*) 30 July 1999 (30.07.99)
International Patent Classification (IPC) or national classification and IPC G07F 7/10, G07C 9/00		
Applicant GIESECKE & DEVRIENT GMBH		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 8 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
06 February 2001 (06.02.01)	01 August 2001 (01.08.2001)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

ernational application No.
PCT/EP00/07122

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☒ the international application as originally filed.

☒ the description, pages _____, as originally filed,
pages _____, filed with the demand,
pages 1-5, filed with the letter of 04 July 2001 (04.07.2001),
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-9, filed with the letter of 04 July 2001 (04.07.2001),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/1, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____
☐ the claims, Nos. _____
☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

ernational application No.
PCT/EP 00/07122

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-3, 5, 6, 8, 9	YES
	Claims	4, 7	NO
Inventive step (IS)	Claims		YES
	Claims	1-9	NO
Industrial applicability (IA)	Claims	1-9	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:
D1: US-A-5 239 166 (GRAVES MARCEL A) 24 August 1993 (1993-08-24)
D2: US-A-5 208 447 (KRUSE DIETRICH) 4 May 1993 (1993-05-04)

2. Independent Claim 1

Document D1, which is the closest prior art, discloses (cf. column 3, line 46 to column 4, line 18) a method for authenticating a user of a data carrier (4) for authorized use of the data carrier and for authenticating a data carrier terminal (3) for authorized access of the data carrier terminal to the storage areas of the data carrier, comprising the following steps:
- presentation of a biometric feature of a user (column 4, lines-8-9),
- comparison of the presented biometric feature with a biometric feature stored on the data carrier (4) (column 4, lines 5-11),

from which the subject matter of Claim 1 differs in that the following steps are first carried out:

- read-out of a secret code from the data carrier by the data carrier terminal, the secret code being stored in a storage location that is accessible only to authorized data carrier terminals and/or the secret code being correctly decodable only by an authorized data carrier terminal,
- presentation of the read out secret code to the user.

The problem to be solved by the present invention can thus be seen as that of making available an alternative method for authenticating a user of a data carrier for authorized use of the data carrier and for authenticating a data carrier terminal which can be directly controlled/carried out by the user.

An authentication of the data carrier terminal also occurs in document D1, but this is carried out independently by the data carrier and the data carrier terminal. However, features a) read-out of a secret code from a storage location that is accessible to authorized data carrier terminals and b) presentation of this code to the user were already used for the same purpose in similar methods for authenticating users and data carrier terminals (cf. document D2, in particular column 2, line 46 to column 3, line 36). If a person skilled in the art wants to achieve the same goal in a method for authenticating users and data carrier terminals according to document D1, this feature could be readily employed to like effect with the subject matter of D1 as well. In this way, the person would arrive at a method for authenticating users and data carrier terminals according to Claim 1 without exercising inventive skill.

The subject matter of Claim 1 thus does not involve an inventive step (PCT Article 33(3)).

3. Independent Claim 4

Document D1 is the closest prior art with respect to the subject matter of Claim 4. It discloses (references in parentheses are to D1):
data carrier (4) for authenticating a terminal for a user and a user for a terminal, comprising
- a first storage area in which a secret code is stored in such a way that the secret code can be read out (6) and displayed (5) by an authorized data carrier terminal (3) (column 4, lines 9-11), and
- a second storage area in which biometric data are stored (column 4, lines 5-9).

The subject matter of Claim 4 is thus not novel (PCT Article 33(2)).

3.1. Even if a particular division or configuration of the two storage areas is intended, the subject matter would still not be considered inventive (PCT Article 33(3)) since many advantageous configurations and the specific use of separate storage areas in the area of chip card and security technology are well-known to a person skilled in the art.

4. Independent Claim 7

Document D1 is the closest prior art with respect to the subject matter of Claim 7. It discloses (references in parentheses are to D1):

authentication system (see column 3, line 46 to column 4, line 18 and Figure 1) comprising a data carrier (4) having storage areas and a data carrier terminal (3) for accessing the storage areas of the data carrier, characterized in that

- the data carrier (4) has a first storage area for storing a secret code and a second storage area for storing biometric data (column 4, lines 5-11);
- the data carrier terminal (3) has a first device, which is authorized to read out (6) the secret code from the storage area and to present (5) the read out secret code on a display, and a second device for reading in biometric data (7), and
- the data carrier has in the data carrier (4) and/or in the data carrier terminal (3) a device for comparing (9) the read-in biometric data with biometric data stored in the second storage area (see also column 4, lines 5-11).

The subject matter of Claim 7 is thus not novel (PCT Article 33(2)).

4.1. As already explained in section 3.1., a particular division or configuration of the two storage areas cannot be considered inventive. Likewise a variation or configuration of the secret code (secret number, random number, PIN, etc.) that lies within the scope of normal practice cannot be considered inventive (PCT Article 33(3)).

5. Dependent Claims 2-3, 5-6 and 8-9

Dependent Claims 2-3, 5-6 and 8-9 contain no additional features which, combined with the features of any claim to which they refer, meet the PCT requirements for novelty and inventive step. The reasons are as follows:

5.1. Claims 2, 5 and 8: The additional use of a personal identification code (PIN) along with the recording of biometric features for authenticating a user of a data carrier has already been suggested in document D1 (see column 4, lines 9-11).

5.2. Claims 3, 6 and 9: Using the finger prints of the user as a biometric feature is only one of a plurality of obvious possibilities from which a person skilled in the art would choose in order to solve the problem of interest without thereby being inventive. In document D1, the use of fingerprints in a similar system and method has already been explicitly suggested.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The feature of the use of an **authorized** data carrier terminal, which was submitted with the letter of 4 July 2001, is not clearly defined (PCT Article 6) and does not contribute to the novelty or inventiveness of the subject matter of the independent claims.

Simply introducing the expression "**authorized** data carrier terminal," even in combination with the description, does not make clear in what way and with which technical means such an **authorized** data carrier terminal should differ from other data carrier terminals. According to the present wording, all data carrier terminals that are suited or equipped to read from the data carrier fall within the category of **authorized** data carrier terminal. However, as a person skilled in the art knows, in many cases a compatibility check is also carried out between the data carrier and the data carrier terminal before the read-out. A positive result of such a check should also be regarded as an authorization of a data carrier terminal. Therefore the feature of an authorized data carrier terminal does not offer any additional technical features that could be considered delimiting in relation to the cited systems and methods in D1 and D2.

Method, data carrier and system for authenticating a user and a terminal

The present invention relates in general to authentication for the use of data carriers such as smart cards and the like, and in particular to an authentication method, a data carrier and an authentication system comprising a data carrier and a terminal.

To prove that a user is actually entitled or authorized to use a smart card or magnetic stripe card, an individual secret number, for example a so-called PIN (personal identification number) is customarily used. The PIN is stored on the card and, after the card has been introduced into a terminal, compared with the PIN entered in the terminal by the user. If comparison is positive the terminal can e.g. access protected areas of the smart card, for example memory areas.

The use of PINs is problematic because the card can be used by anyone with knowledge of the PIN. The card is thus not bound to the actual card holder but to the PIN holder. Voluntary or involuntary transmission of the PIN thus makes it possible to abuse the card. PINs are also unsafe insofar as they can be forgotten, on the one hand, and spied out, on the other hand.

Even when an authorized user has identified himself by entering his PIN, the system is only partially authorized - that is, the user with respect to the card and to the terminal. There is no authorization of the terminal with respect to the card or to the user. If the terminal is fake there is a danger of the PIN being spied out by the fake terminal. The PIN alone therefore does not constitute sufficient protection because there is no authentication of the terminal with respect to the card or to the user.

The present invention is based on the problem of making the authentication process safer. In particular, the problem underlying the invention is to propose an authentication method, an authentication system comprising data carrier and terminal, and a data carrier for authenticating both the user and the terminal, thereby permitting the user's individual authorization and the authenticity of the terminal to be checked.

This problem is solved according to the invention by an authentication method, a data carrier and an authentication system according to the independent claims.

The subclaims state advantageous embodiments of the invention.

The inventive solution is based on the idea that the authentication process can be made safer if the authenticity of the terminal is first checked and the terminal is then presented with biometric data of the user. Biometric data, such as a fingerprint or the like, are clearly user-specific, unlike a PIN. The prior check of the terminal's authenticity guarantees that the sensitive, user-specific biometric data cannot be spied out. The terminal's authenticity is checked by a secret code permanently stored on the data carrier and known only to the user being read by the terminal and displayed to the user. Only if the secret code is displayed correctly does the user present the biometric feature to the terminal to identify himself as an authorized user to the terminal and the data carrier. The secret code can be stored on the data carrier on a memory location that can be accessed only by authorized terminals and/or be decrypted correctly only by an authorized terminal.

After the terminal has been authenticated, user-unique authentication with respect to the data carrier and to the terminal is obtained by presentation of the user-specific biometric feature and comparison of the data detected from the biometric feature with biometric data stored on the data carrier, in contrast to PIN comparison.

In addition to biometric authentication of the user, a PIN authentication of the user can be effected by entry of a PIN and comparison of the entered PIN with the PIN stored on the data carrier.

The invention will be set forth in the following by way of example with reference to the single figure.

The authentication process shown in the figure includes three steps, of which the second step can be omitted.

In the first step, terminal *T* reads a secret code (*CODE*) from a first memory area of data carrier *C*, for example a smart card, and presents said *CODE* to user *U*. *CODE* is stored on smart card *C* for example on a protected-access memory location and/or in encrypted form, so that *CODE* can only be read and displayed to user *U* by "real" terminal *T* which either has access authority or knows the decryption algorithm.

If user *U* recognizes *CODE* read by terminal *T* as his secret code, he will perform the further authentication steps. In the shown case, he will first enter his PIN in terminal *T*. The PIN is then transmitted, preferably in encrypted form, to smart card *C*

where it is decrypted and compared with a PIN stored on smart card *C*, and the result of comparison is then reported to terminal *T*. The data transfer, in particular the transfer of *CODE*, the PIN and biometric data *BIO* to be described below, is preferably effected in encrypted form in order to protect said sensitive data from being spied out.

If the PIN comparison was positive ("*OK*"), terminal *T* continues the authentication process by now effecting the user-unique authentication by means of the user's biometric features. The user presents terminal *T* with a biometric feature, for example a fingerprint or the iris of an eye. The biometric feature is detected by terminal *T* and converted into biometric data *BIO* which are transmitted, preferably in encrypted form, to smart card *C*. There, the user's read biometric data are compared with biometric data stored on smart card *C*. In the case of a positive comparison ("*OK*"), terminal *T* is enabled for the entry of further user commands.

Claims

1. A method for authenticating a user (*U*) of a data carrier (*C*) for authorized use of the data carrier and for authenticating a data carrier terminal (*T*) for authorized accessing by the data carrier terminal of memory areas of the data carrier, comprising the following steps:
   - reading a secret code (*CODE*) from the data carrier (*C*) by the data carrier terminal (*T*),
   - presenting the read secret code (*CODE*) to the user (*U*),
   - presenting a biometric feature (*BIO*) of a user (*U*),
   - comparing the presented biometric feature (*BIO*) with a biometric feature stored on the data carrier (*C*).
2. A method according to claim 1, characterized in that a PIN is in addition presented to the terminal (*T*), being compared with a PIN stored on the data carrier (*C*).
3. A method according to claim 1 or 2, characterized in that a fingerprint of a user (*U*) is used as the biometric feature (*BIO*).
4. A data carrier (*C*) for authenticating a terminal with respect to a user and the user with respect to the data carrier, comprising a first memory area in which a secret code (*CODE*) is stored such that the secret code can be read and displayed by a data carrier terminal (*T*), and a second memory area in which biometric data are stored.
5. A data carrier according to claim 4, characterized in that a PIN is stored in a third memory area.
6. A data carrier according to either of claims 4 and 5, characterized in that the biometric data are generated by a fingerprint.
7. An authentication system comprising a data carrier (*C*) with memory areas and a data carrier terminal (*T*) for accessing the memory areas of the data carrier, characterized in that
   - the data carrier (*C*) has a first memory area for storing a secret code (*CODE*) and a second memory area for storing biometric data,

- the data carrier terminal (*T*) has a first device for reading the secret code (*CODE*) from the first memory area and presenting the read secret code on a display, and a second device for reading biometric data (*BIO*), and
- a device for comparing the read biometric data (*BIO*) with biometric data stored in the second memory area in the data carrier (*C*) and/or in the terminal (*T*).

8. An authentication system according to claim 7, characterized in that the data carrier (*C*) has a third memory area for storing a PIN.

9. An authentication system according to claim 7 or 8, characterized in that the stored biometric data are generated by a fingerprint.

Abstract

In connection with the use of data carriers such as smart cards *C* and the like, it is proposed that terminal *T* in which smart card *C* is processed is first authenticated with respect to user *U* and user *U* is then authenticated with respect to data carrier *C* and terminal *T*. Authentication of the terminal with respect to user *U* is effected by reading *CODE* from data carrier *C* and presenting read *CODE* to user *U* who ranks presented *CODE* as correct or false. If terminal *T* has presented correct *CODE*, user *U* authenticates himself with respect to smart card *C* and terminal *T* by presenting biometric feature *BIO*, for example his fingerprint. This procedure ensures that biometric feature *BIO* of user *U* cannot be spied out by fake terminal *T*.

Verfahren, Datenträger sowie System zur Authentisierung eines Benutzers und eines Endgeräts

Die vorliegende Erfindung betrifft allgemein die Authentisierung bei der Benutzung von Datenträgern wie Chipkarten und dergleichen, und insbesondere ein Authentisierungsverfahren, einen Datenträger sowie ein Authentisierungssystem umfassend einen Datenträger und ein Endgerät (Terminal).

Zum Nachweis, daß ein Benutzer zur Benutzung einer Chip- oder Magnetstreifenkarte tatsächlich berechtigt bzw. autorisiert ist, dient üblicherweise eine individuelle Geheimzahl, beispielsweise eine sogenannte PIN (Persönliche Identifizierungs Nummer). Die PIN ist auf der Karte gespeichert und wird, nachdem die Karte in ein Endgerät eingeführt worden ist, mit der dem Endgerät von dem Benutzer angegebenen PIN verglichen. Ist der Vergleich positiv, so kann vom Endgerät z. B. auf geschützte Bereiche der Chipkarte, beispielsweise Speicherbereiche, zugegriffen werden.

Die Benutzung von PINs ist problematisch, weil die Karte in Kenntnis der PIN von jedermann benutzt werden kann. Die Karte ist also nicht an den eigentlichen Karteninhaber, sondern an den PIN-Inhaber gebunden. Durch freiwillige oder unfreiwillige Weitergabe der PIN ist somit ein Mißbrauch der Karte möglich. PINs sind auch insofern unsicher, als sie einerseits vergessen und andererseits ausgespäht werden können.

Selbst wenn sich ein berechtigter Benutzer durch Eingabe seiner PIN ausgewiesen hat, ist das System nur teilweise autorisiert - nämlich der Benutzer gegenüber der Karte beziehungsweise dem Endgerät. Eine Autorisierung des Endgeräts gegenüber der Karte oder dem Benutzer findet nicht statt. Handelt es sich um ein gefälschtes Endgerät, so besteht die Gefahr, daß die PIN mittels dem gefälschten Endgerät ausgespäht wird. Die PIN allein stellt

daher keine ausreichende Sicherung dar, weil eine Authentisierung des Endgeräts gegenüber der Karte bzw. gegenüber dem Benutzer fehlt.

Der vorliegenden Erfindung liegt die Aufgabe zugrunde, den Authentisierungsvorgang sicherer zu gestalten. Insbesondere besteht die der Erfindung zugrunde liegende Aufgabe darin, ein Authentisierungsverfahren, ein Authentisierungssystem bestehend aus Datenträger und Endgerät und einen Datenträger zur Authentisierung sowohl des Benutzers als auch des Terminals vorzuschlagen, wodurch die individuelle Berechtigung des Benutzers und die Echtheit des Terminals überprüfbar sind.

Diese Aufgabe wird erfindungsgemäß durch ein Authentisierungsverfahren, einen Datenträger und ein Authentisierungssystem gemäß den nebengeordneten Ansprüchen gelöst.

In den Unteransprüchen sind vorteilhafte Ausgestaltungen der Erfindung angegeben.

Der erfindungsgemäßen Lösung liegt der Gedanke zugrunde, daß der Authentisierungsvorgang sicherer gestaltet werden kann, wenn zunächst die Echtheit des Terminals geprüft wird und dem Terminal anschließend biometrische Daten des Benutzers präsentiert werden. Biometrische Daten, wie ein Fingerabdruck oder dergleichen, sind im Gegensatz zu einer PIN eindeutig benutzerspezifisch. Durch das vorherige Prüfen der Echtheit des Terminals wird gewährleistet, daß ein Ausspähen der sensiblen, benutzerspezifischen biometrischen Daten verhindert wird. Das Prüfen der Echtheit des Endgeräts geschieht in der Weise, daß ein auf dem Datenträger fest gespeicherter Geheimcode, der nur dem Benutzer bekannt ist, von dem Endgerät ausgelesen und dem Benutzer angezeigt wird. Nur wenn der Geheimcode korrekt ange-

zeigt wird, wird der Benutzer dem Endgerät das biometrische Merkmal präsentieren, um sich gegenüber dem Endgerät bzw. dem Datenträger als berechtigter Benutzer auszuweisen. Der Geheimcode kann auf dem Datenträger auf einem nur durch autorisierte Endgeräte zugreifbaren Speicherplatz gespeichert sein und/oder nur von einem autorisierten Endgerät korrekt entschlüsselt werden.

Nachdem die Authentisierung des Terminals erfolgt ist, wird durch Präsentieren des benutzerspezifischen biometrischen Merkmals und Vergleich der von dem biometrischen Merkmal erfaßten Daten mit auf dem Datenträger gespeicherten biometrischen Daten, im Gegensatz zum PIN-Vergleich, eine benutzerindividuelle Authentisierung gegenüber dem Datenträger bzw. dem Endgerät erreicht.

Zusätzlich zur biometrischen Authentisierung des Benutzers kann eine PIN-Authentisierung des Benutzers durch Eingabe einer PIN und Vergleich der eingegebenen PIN mit auf dem Datenträger gespeicherter PIN erfolgen.

Die Erfindung wird nachfolgend beispielhaft anhand der einzigen Figur dargestellt.

Der in der Figur dargestellte Authentisierungsvorgang umfaßt drei Schritte, von denen der zweite Schritt auch entfallen kann.

Im ersten Schritt liest ein Endgerät T (Terminal) von einem ersten Speicherbereich eines Datenträgers C, beispielsweise einer Chipkarte, einen Geheimcode (CODE) aus und präsentiert diesen CODE dem Benutzer U (User). Der CODE ist auf der Chipkarte C beispielsweise auf einem zugriffsgeschützten Speicherplatz und/oder in verschlüsselter Form abgespeichert, so daß der

CODE nur von einem "echten" Terminal T, das entweder zugriffsberechtigt ist oder den Entschlüsselungsalgorithmus kennt, ausgelesen und dem Benutzer U angezeigt werden kann.

Wenn der Benutzer U den von dem Terminal T ausgelesenen CODE als seinen Geheimcode wiedererkennt, wird er die weiteren Authentisierungsschritte vornehmen. Im dargestellten Fall wird er dem Terminal T zunächst seine PIN angeben. Die PIN wird dann, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet, wo sie entschlüsselt und mit einer auf der Chipkarte C abgespeicherten PIN verglichen wird, und dem Terminal T wird anschließend das Ergebnis des Vergleichs mitgeteilt. Der Datentransfer, insbesondere der Transfer des CODE's, der PIN und der nachfolgend noch zu beschreibenden biometrischen Daten BIO erfolgt vorzugsweise in verschlüsselter Form, um ein Ausspähen dieser sensiblen Daten zu erschweren.

Sofern der PIN-Vergleich positiv war ("OK"), führt das Terminal T den Authentisierungsprozeß fort, indem nunmehr die benutzerindividuelle Authentisierung mittels biometrischer Merkmale des Benutzers erfolgt. Dazu präsentiert der Benutzer dem Terminal T ein biometrisches Merkmal, beispielsweise einen Fingerabdruck oder die Iris eines Auges. Das biometrische Merkmal wird vom Terminal T erfaßt und in biometrische Daten BIO umgewandelt, die, vorzugsweise in verschlüsselter Form, an die Chipkarte C weitergeleitet werden. Dort werden die eingelesenen biometrischen Daten des Benutzers mit auf der Chipkarte C gespeicherten biometrischen Daten verglichen. Im Falle eines positiven Vergleichs ("OK") wird das Terminal T für die Eingabe weiterer Benutzerkommandos freigegeben.

Patentansprüche

1. Verfahren zum Authentisieren eines Benutzers (U) eines Datenträgers (C) zur berechtigten Benutzung des Datenträgers und zum Authentisieren eines Datenträgerendgerätes (T) zum berechtigten Zugreifen des Datenträgerendgerätes auf Speicherbereiche des Datenträgers, umfassend folgenden Schritte:

- Auslesen eines Geheimcodes (CODE) von dem Datenträger (C) durch das Datenträgerendgerät (T),
- Präsentieren des ausgelesenen Geheimcodes (CODE) gegenüber dem Benutzer (U),
- Präsentieren eines biometrischen Merkmals (BIO) eines Benutzers (U),
- Vergleichen des präsentierten biometrischen Merkmals (BIO) mit einem auf dem Datenträger (C) gespeicherten biometrischen Merkmal.

2. Verfahren nach Anspruch 1, **dadurch gekennzeichnet,** daß dem Terminal (T) desweiteren eine PIN präsentiert wird, die mit einer auf dem Datenträger (C) gespeicherten PIN verglichen wird.

3. Verfahren nach Anspruch 1 oder 2, **dadurch gekennzeichnet,** daß als biometrisches Merkmal (BIO) ein Fingerabdruck eines Benutzers (U) verwendet wird.

4. Datenträger (C) zur Authentisierung eines Endgeräts gegenüber einem Benutzer und des Benutzers gegenüber dem Datenträger, umfassend einen ersten Speicherbereich, in dem ein Geheimcode (CODE) derart abgespeichert ist, daß der Geheimcode von einem Datenträgerendgerät (T) auslesbar und

anzeigbar ist, und einen zweiten Speicherbereich, in dem biometrische Daten abgespeichert sind.

5. Datenträger nach Anspruch 4, **dadurch gekennzeichnet,** daß in einem dritten Speicherbereich eine PIN abgespeichert ist.

6. Datenträger nach einem der Ansprüche 4 oder 5, **dadurch gekennzeichnet,** daß durch biometrischen Daten durch einen Fingerabdruck generiert werden.

7. Authentisierungssystem umfassend einen Datenträger (C) mit Speicherbereichen und ein Datenträgerendgerät (T) zum Zugreifen auf die Speicherbereiche des Datenträgers, **dadurch gekennzeichnet,** daß

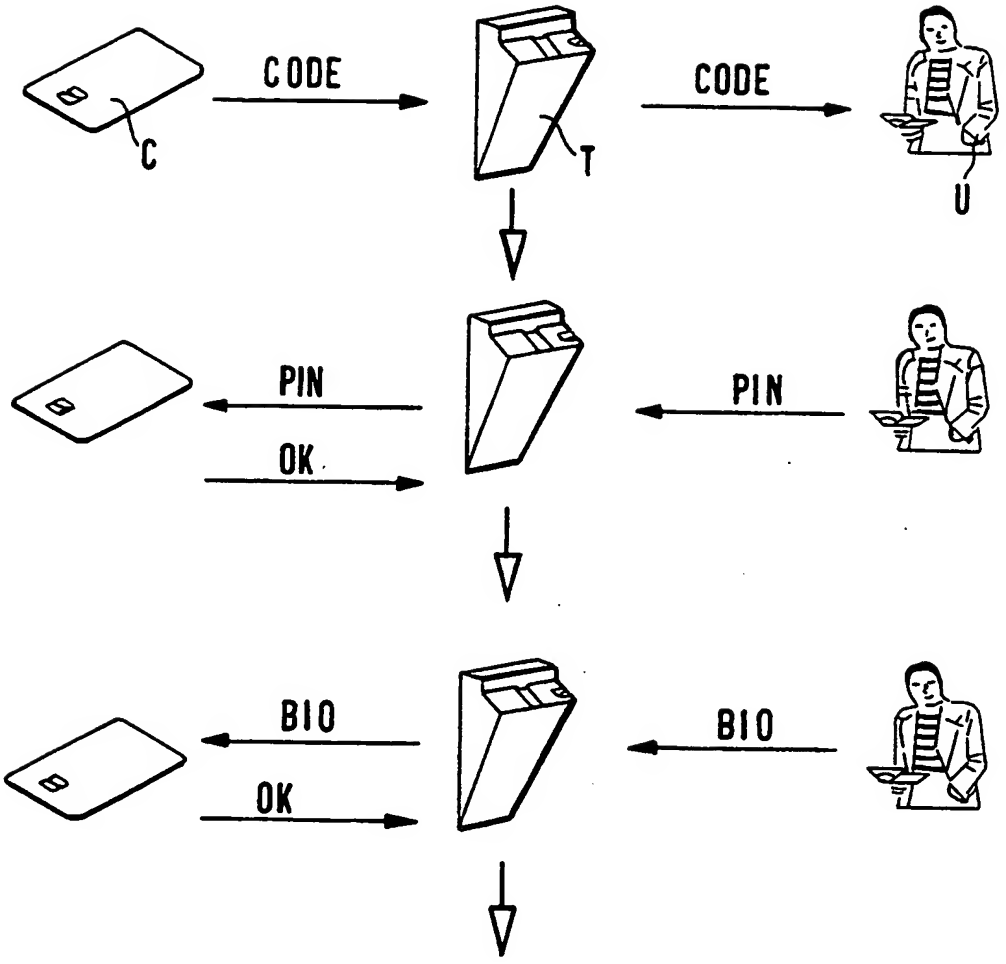
- der Datenträger (C) einen ersten Speicherbereich für die Speicherung eines Geheimcodes (CODE) und einen zweiten Speicherbereich für die Speicherung biometrischer Daten,
- das Datenträgerendgerät (T) eine erste Einrichtung zum Auslesen des Geheimcodes (CODE) aus dem ersten Speicherbereich und Präsentieren des ausgelesenen Geheimcodes auf einem Display, sowie eine zweite Einrichtung zum Einlesen biometrischer Daten (BIO), und
- eine Einrichtung zum Vergleichen der eingelesenen biometrischen Daten (BIO) mit im zweiten Speicherbereich gespeicherten biometrischen Daten im Datenträger (C) und/oder im Datenendgerät (T).

aufweist.

8. Authentisierungssystem nach Anspruch 7, **dadurch gekennzeichnet,** daß der Datenträger (C) einen dritten Speicherbereich für die Speicherung einer PIN aufweist.

9. Authentisierungssystem nach Anspruch 7 oder 8, **dadurch gekennzeichnet,** daß die gespeicherten biometrischen Daten durch einen Fingerabdruck generiert werden.

1 / 1



Interr ...l Application No
PCT/ 00/07122

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10 G07C9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 208 447 A (KRUSE DIETRICH) 4 May 1993 (1993-05-04) abstract column 2, line 46 -column 3, line 36	1-9
Y	US 5 239 166 A (GRAVES MARCEL A) 24 August 1993 (1993-08-24) abstract column 3, line 46 -column 4, line 19; claim 1	1-9
A	US 5 721 781 A (DEO VINAY ET AL) 24 February 1998 (1998-02-24) abstract column 9, line 49 -column 10, line 30; figures 7,8	1-3

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 October 2000	03/11/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Teutloff, H

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int[illegible]nal Application No
[illegible]/EP 00/07122

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 875 868 A (PITNEY BOWES) 4 November 1998 (1998-11-04)	

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5208447 A	04-05-1993	AT 109293 T	15-08-1994
		DE 59006559 D	01-09-1994
		EP 0400441 A	05-12-1990
		ES 2057264 T	16-10-1994
US 5239166 A	24-08-1993	CA 1326304 A	18-01-1994
		AT 125054 T	15-07-1995
		AU 633534 B	04-02-1993
		AU 4781590 A	26-07-1990
		DE 69020746 D	17-08-1995
		EP 0379333 A	25-07-1990
		JP 2271466 A	06-11-1990
		NZ 232106 A	26-05-1993
		NZ 244768 A	26-05-1993
US 5721781 A	24-02-1998	NONE	
EP 0875868 A	04-11-1998	CA 2231210 A	04-09-1998

Internales Aktenzeichen
EP 00/07122

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	EP 0 875 868 A (PITNEY BOWES) 4. November 1998 (1998-11-04)	

Angaben zu Veröffentlichung ., die z* en Patentfamilie gehören

Intern. ...s Aktenzeichen
PCT, 00/07122

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5208447 A	04-05-1993	AT 109293 T	15-08-1994
		DE 59006559 D	01-09-1994
		EP 0400441 A	05-12-1990
		ES 2057264 T	16-10-1994
US 5239166 A	24-08-1993	CA 1326304 A	18-01-1994
		AT 125054 T	15-07-1995
		AU 633534 B	04-02-1993
		AU 4781590 A	26-07-1990
		DE 69020746 D	17-08-1995
		EP 0379333 A	25-07-1990
		JP 2271466 A	06-11-1990
		NZ 232106 A	26-05-1993
		NZ 244768 A	26-05-1993
US 5721781 A	24-02-1998	KEINE	
EP 0875868 A	04-11-1998	CA 2231210 A	04-09-1998